

# A Corollary of Hamada and Ohmori's on Group Law over BIBD

Arnaud Bannier<sup>1</sup>, Johann Barbier<sup>2</sup>, Eric Filiol<sup>1</sup>, and Pierre Castel<sup>2</sup>

<sup>1</sup> ESIEA - CVO Lab. F-53 000 Laval FRANCE

<sup>2</sup> ARX Arceo - Security Lab. - F-35 580 Guichen FRANCE  
 arnaud.bannier@esiea-ouest.fr

**Abstract.** In this note, we present an interesting corollary of a theorem of Hamada and Ohmori. We prove that the complementary of  $PG(n, 2)$  is the only design, up to an isomorphism, whose blocks form a group for the symmetric difference.

**Keywords:** symmetric BIBD, symmetric difference, rank of incidence matrix

## Introduction

The construction and the existence of BIBDs of given  $(v, k, \lambda)$  parameters is an open problem [2, pp 36–57]. Different works exhibit necessary conditions on these parameters (for example, the well-known Fisher's inequality [3]), but without any additional hypothesis, finding sufficient conditions is difficult. A more natural approach consists in adapting algebraic structures to find infinite families of BIBDs. In this way, properties of combinatorial designs can be equivalent to algebraic ones. For instance, Hadamard matrices are known to be equivalent to  $(4n - 1, 2n - 1, n - 1)$ -BIBDs [1] and so provide families of BIBDs [9]. One of the most widespread strategies relies on group structures [1].

A first approach consists in fixing an automorphism group to deduce associated designs [8]. Another one relies on finding a subset of a finite group with fixed properties called a *difference set*. The elements of the group are the points of the design, the subset and its translates are the blocks of the design [5][1, chapter 6]. It is also natural to consider design blocks as elements of a finite group.

Some group laws on blocks of a design have already been highlighted in the literature. In his paper [6], Kantor gave one of the most relevant examples. A symmetric BIBD satisfies the *symmetric difference property* (SDP) if for any three blocks  $B, C, D$  then  $B \Delta C \Delta D$  is either a block or the complement of a block (where  $\Delta$  denote the symmetric difference). Kantor investigated such designs and proved [6, Theorem 3] that a group law can be defined on their blocks as follows. Choose a block  $B$  (the neutral element). For all blocks  $X$  and  $Y$ , define  $X + Y$  as  $B \Delta X \Delta Y$  or its complement depending on which of the two results is a block. With this addition, the blocks form an elementary abelian

2-group. Kantor also gave the family  $\mathcal{S}^\epsilon(2m)$  of SDP-designs and proved that any other family of SDP-designs must have the same parameters.

Another example is provided by Kimberley [7]. Let  $(X, \mathcal{B})$  be a Hadamard 3-design. Then, the complement of any block is another block. A block  $B$  is said to be *good* if for all block  $C$  distinct from  $B$  and its complement  $\overline{B}$ , the symmetric difference  $B \Delta C$  is again a block. Remark that the original definition of Kimberley is different but equivalent to this one for the Hadamard 3-designs. If  $B$  is a good block, then  $\overline{B}$  is also a good block and  $\{B, \overline{B}\}$  is a *good block class*. Let  $\mathcal{G}$  be the set of all good block classes and let  $\mathcal{H}$  be the set  $\mathcal{G} \cup \{\{X, \emptyset\}\}$ . Define the binary operation  $\circ$  on  $\mathcal{H}$  by  $\{B, \overline{B}\} \circ \{C, \overline{C}\} = \{B \Delta C, \overline{B \Delta C}\}$ . Then,  $\mathcal{H}$  is an elementary abelian 2-group under the operation  $\circ$ , see [7, Lemma 4.8].

Here, we propose an original approach similar with [6, 7] which provides BIBDs whose blocks form a group for the symmetric difference. We show necessary conditions on parameters to provide BIBDs with such a structure and prove that they are sufficient with a result of Hamada and Ohmori. We emphasize that all such designs have been found.

Initially, the additional group structure allowed us to construct these designs and prove their uniqueness up to an isomorphism. This construction was in fact equivalent to that of Sylvester [10]. Then, we found that our main result can be seen as a corollary of a theorem of Hamada and Ohmori [4, Theorem 4.2]. It is in this perspective that we present this paper.

The paper is organized as follows: first, we recall basic definitions and notations. Then, we study the necessary conditions to provide the BIBDs with a group structure. We conclude using the result Hamada and Ohmori.

## 1 Basic Notations and Definitions

**Definition 1.** Let  $X$  be a finite set with  $v$  elements called points and  $\mathcal{B}$  be a set of subsets of  $X$  called blocks. The pair  $(X, \mathcal{B})$  is said to be a simple  $(v, k, \lambda)$  balanced incomplete block design (or a simple  $(v, k, \lambda)$ -BIBD for short) if all the blocks contain exactly  $k$  points and if every pair of distinct points is contained in exactly  $\lambda$  blocks. It is also required that  $v > k \geq 2$ . Such a design is said symmetric, and denoted SBIBD, if the number of points is equal to the number of blocks, or equivalently, if the cardinal of the intersection of two blocks is constant [1, Corollary II.3.3].

It is well known that the equality  $\lambda(v-1) = k(k-1)$  holds in any  $(v, k, \lambda)$ -SBIBD [1, Definition II.3.1]. Let  $(X, \mathcal{B})$  be a simple  $(v, k, \lambda)$ -BIBD. Write  $X = \{x_1, \dots, x_v\}$  and  $\mathcal{B} = \{B_1, \dots, B_b\}$ . The *incidence matrix* of  $(X, \mathcal{B})$  (for this order) is the matrix  $M = (m_{i,j})_{\substack{1 \leq i \leq v \\ 1 \leq j \leq b}}$  defined by

$$m_{i,j} = \begin{cases} 1 & \text{if } x_i \in B_j, \\ 0 & \text{if } x_i \notin B_j. \end{cases}$$

## 2 Necessary and Sufficient Conditions

Let  $(X, \mathcal{B})$  be a simple  $(v, k, \lambda)$ -BIBD. The goal of this paper is to endow  $\mathcal{B}$  with a group law. As  $\mathcal{B}$  is included in the power set  $\mathcal{P}(X)$  of  $X$ , choosing a binary operation  $*$  such that  $(\mathcal{B}, *)$  is a subgroup of  $(\mathcal{P}(X), *)$  is natural. Among all classical binary operations<sup>3</sup> on  $\mathcal{P}(X)$ , the symmetric difference  $\Delta$  is the only one which gives rise to a group. The empty set  $\emptyset$ , the neutral element of  $(\mathcal{P}(X), \Delta)$ , is never in  $\mathcal{B}$ . Thus, we define<sup>4</sup>  $\mathcal{B} = (\mathcal{B} \cup \{\emptyset\}, \Delta)$ . The purpose of this section is to study the conditions over the parameters  $(v, k, \lambda)$  such that  $\mathcal{B}$  is a group.

**Lemma 2.** *Assuming that  $\mathcal{B}$  is a group, the design  $(X, \mathcal{B})$  is a symmetric  $(4\lambda - 1, 2\lambda, \lambda)$ -BIBD.*

*Proof.* Let  $B, B'$  be two distinct elements of  $\mathcal{B}$ . By definition, each block of  $\mathcal{B}$  contains exactly  $k$  points. As  $B \Delta B'$  is an element of  $\mathcal{B}$ ,  $|B \Delta B'| = k$ . Since

$$|B \Delta B'| = |B| + |B'| - 2|B \cap B'| = 2k - 2|B \cap B'|,$$

the equality  $2|B \cap B'| = k$  holds. Noting that the cardinal of the intersection of two blocks is constant,  $(X, \mathcal{B})$  is a symmetric BIBD and  $|B \cap B'| = \lambda$ . Thus, we have  $2\lambda = k$ . From the equality  $\lambda(v - 1) = k(k - 1)$ , it follows that

$$v = \frac{k(k - 1)}{\lambda} + 1 = \frac{2\lambda(2\lambda - 1)}{\lambda} + 1 = 4\lambda - 1.$$

Hence,  $(X, \mathcal{B})$  is a  $(4\lambda - 1, 2\lambda, \lambda)$ -SBIBD.  $\square$

Write  $X = \{x_1, \dots, x_v\}$ ,  $\mathcal{B} = \{B_1, \dots, B_b\}$  and let  $M$  be the incidence matrix of  $(X, \mathcal{B})$ . Let  $C_1, \dots, C_b$  be its columns, seen as elements of  $\mathbb{F}_2^b$  and define  $C_0 = (0, \dots, 0) \in \mathbb{F}_2^b$ . The blocks  $B_i$  and  $B_j$  ( $1 \leq i, j \leq b$ ,  $i \neq j$ ) are represented respectively by  $C_i$  and  $C_j$ . It is easily seen that  $B_i \Delta B_j$  is represented by  $C_i + C_j$  and  $B_i \Delta B_i = \emptyset$  by  $C_0$ . Define  $\mathcal{C} = (\{C_0, C_1, \dots, C_b\}, +)$ . Consequently,  $\mathcal{B}$  is a group if, and only if  $\mathcal{C}$  is a group. If this is the case,  $\mathcal{C}$  has an additional structure of  $\mathbb{F}_2$ -vector space.

**Lemma 3.** *Let  $n$  denote the rank of  $M$ . Then  $\mathcal{B}$  is a group if, and only if  $(X, \mathcal{B})$  is a  $(2^n - 1, 2^{n-1}, 2^{n-2})$ -SBIBD.*

*Proof.* By definition,  $n$  is the dimension of the subspace  $\text{span}(\mathcal{C})$  of  $\mathbb{F}_2^{2^n-1}$ . Assume that  $\mathcal{B}$  is a group. It follows that  $\mathcal{C}$  equals  $\text{span}(\mathcal{C})$ , so  $\mathcal{C}$  has  $2^n$  elements and the number  $b$  of blocks equals  $2^n - 1$ . From Lemma 2, we have  $v = b = 4\lambda - 1$  and  $k = 2\lambda$ . Then  $2^n - 1 = 4\lambda - 1$ , that is  $\lambda = 2^{n-2}$ . Consequently,  $(X, \mathcal{B})$  is a  $(2^n - 1, 2^{n-1}, 2^{n-2})$ -SBIBD.

Conversely, assume that  $(X, \mathcal{B})$  is a  $(2^n - 1, 2^{n-1}, 2^{n-2})$ -SBIBD. Of course,  $\mathcal{C} \subset \text{span}(\mathcal{C})$  and  $|\mathcal{C}| = |\text{span}(\mathcal{C})| = 2^n$ . It follows that  $\mathcal{C}$  is a vector space and  $\mathcal{B}$  is a group.  $\square$

<sup>3</sup> By classical, we mean  $\cup$ ,  $\cap$ ,  $\Delta$  and  $\setminus$ .

<sup>4</sup> We should define  $\mathcal{B} = (\mathcal{B} \cup \{\emptyset\}, \tilde{\Delta})$  where  $\tilde{\Delta}$  is the restriction of  $\Delta$  on  $\{(B, C) \in (\mathcal{B} \cup \{\emptyset\})^2 \mid B \Delta C \in \mathcal{B} \cup \{\emptyset\}\}$ .

Let us now consider the following theorem due to Hamada and Ohmori [4, Theorem 4.2].

**Theorem 4.** *Let  $D$  be a  $(2^n - 1, 2^{n-1}, 2^{n-2})$ -SBIBD and let  $N$  be an incidence matrix of  $D$ . Then,*

$$\text{rank}_2(M) \geq n$$

*and the equality is attained when and only when the design  $D$  is isomorphic with the complementary design of  $PG(n - 1, 2)$ .*

Now, we can state the main result of this note, which is a direct consequence of Lemma 3 and Theorem 4.

**Corollary 5.** *Let  $n$  denote the rank of  $M$ . Then the complementary of  $PG(n - 1, 2)$  is the only BIBD up to isomorphism such that  $\mathcal{B}$  is a group.*

### 3 Conclusion

In this paper, we have considered combinatorial designs provided with a group law inherent to the blocks, namely the symmetric difference. We began by reviewing necessary conditions and found that these designs must have the parameters  $(2^n - 1, 2^{n-1}, 2^{n-2})$ . Using a result due to Hamada and Ohmori, we proved that the complementary of  $PG(n - 1, 2)$  is the only one with this property, up to an isomorphism.

### References

1. Thomas Beth, Dieter Jungnickel, and Hanfried Lenz, *Design theory. 1*, vol. 69, Cambridge University Press, 1999.
2. Charles J Colbourn and Jeffrey H Dinitz, *Handbook of combinatorial designs*, CRC press, 2010.
3. Ronald Aylmer Fisher, *An examination of the different possible solutions of a problem in incomplete blocks*, Annals of Eugenics **10** (1940), no. 1, 52–75.
4. N Hamada and H Ohmori, *On the BIB design having the minimum  $p$ -rank*, Journal of Combinatorial Theory, Series A **18** (1975), no. 2, 131–140.
5. Dieter Jungnickel, A Pott, and KW Smith, *Difference sets*, Contemporary design theory: a collection of surveys (1992), 241–324.
6. William M Kantor, *Symplectic groups, symmetric designs and line ovals*, J. Algebra **33** (1975), no. 197, 5.
7. Marion E Kimberley, *On the construction of certain hadamard designs*, Mathematische Zeitschrift **119** (1971), no. 1, 41–59.
8. Earl S Kramer and Dale M Mesner,  *$t$ -designs on hypergraphs*, Discrete Mathematics **15** (1976), no. 3, 263–296.
9. Jennifer Seberry and Mieko Yamada, *Hadamard matrices, sequences, and block designs*, (1992).
10. James Joseph Sylvester, *Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to newton's rule, ornamental tile-work, and the theory of numbers*, The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **34** (1867), no. 232, 461–475.